122 or a DRSF1 server **124** controlling a D2D area where the UE1 is located, or an eNB2 **142** or a DRSF2 server **144** controlling a D2D area where the UE2 is located. Although FIG. **1** illustrates the DRSF servers **124**, **144** as an entity separate and distinct from any of the access network elements, in practice the function of the server **124**, **144** may be incorporated in any apparatus (for example, in the eNB **122**, **142** respectively) of the radio access network. The eNBs and DRSFs may communicate with each another directly or via some intermediate node, such as a MME.

[0037] Referring to FIG. **2**, UE1 **110**A is camping on eNB1/DRSF1 at **210**A, and then registered to eNB1 or DRSF1 for potential D2D services. As illustrated in FIG. **1**, eNB1 or DRSF1 controls a D2D area where UE1 is currently located in, for D2D services in this D2D area. This registration may be performed as D2D area registration. With the registration, the eNB1/DRSF1 may establish a security context of UE1 for securing D2D services of UE1. In this regard, the eNB1/DRSF1 may store and maintain an association between a UE-specific key (denoted as $K_{d2d\text{-}UE1}$) of the UE1 with the identity (e.g. UE1's S-TMSI) of UE1. The key $K_{d2d\text{-}UE1}$ may be shared between the UE1 and the eNB1/DRSF1. For example, $K_{d2d\text{-}UE1}$ may be originally generated at the UE1 and the MME **132**, based on a NAS key (e.g. K_{asme} of UE1) shared between the UE1 and the MME **132**, and may be sent from the MME to the eNB1/DRSF1, for example during a registration of the UE1 to the eNB1/DRSF1. In some exemplary embodiments, the security context of UE1 including $K_{d2d\text{-}UE1}$, may be transferred from an eNB/DRSF controlling a D2D area where UE1 is previously located in, to the current eNB1/DRSF1. Details of the transfer of security context will be discussed later with reference to FIG. **3**.

[0038] In some embodiments, UE1 may stay in RRC (Radio Resource Control) idle mode after camping on eNB1/DRSF1. For example, UE1 may stay in RRC idle mode as specified in LTE protocols. Then, there may be no RRC connection established between the UE1 and the eNB1. As a device capable of D2D communication, UE1 may broadcast notifications for D2D services to its adjacent D2D UEs when it wants D2D communications, even if it stays in RRC idle mode. For example at **215**, UE1 may broadcast a notification for D2D services, for example in a D2D beacon. The notification identifies UE1 as the originator of the D2D services with UE1's identity. For example, the notification may indicate UE1's own S-IMSI (Short-Temporary Mobile Subscriber Identity), the D2D services, . . . , and so on. Especially, UE1 also broadcasts the identification of a D2D area where UE1 is currently located in. For example, the notification may also comprise a cell ID of the cell UE1 is currently camping on. Although as illustrated in FIG. **2**, UE1 is in idle mode while broadcast the notification, the notification may also be broadcasted while UE1 is in RRC connected mode.

[0039] Then, one or more adjacent D2D UEs (e.g. UE2 **110**B) may detect the D2D beacons broadcasted from UE1, and decide to establish a D2D connection with UE1. From the notification in detected D2D beacons, UE2 may obtain the identity (e.g. S-TMSI) of UE1 and the D2D area where UE1 is currently located in, and trigger a procedure to request security keys for protecting the D2D communication to be performed between UE1 and UE2. As illustrated at block **225**, UE2 **110**B may send a request message for the security keys to its serving eNB/DRSF, i.e. eNB2/DRSF2, including the S-TMSI of UE1 and the identification (e.g. cell ID of eNB2) of the D2D area where UE1 is currently located in. The request message may be transmitted through a RRC connection between UE2 and the eNB **142**. In some exemplary embodiments, UE2 may have an activate RRC connection with the eNB2 or DRSF2 at the moment of deciding to establish a D2D communication connection with UE1. In the case that there is no RRC connection between UE2 and the eNB2/DRSF2, UE2 may initiate a RRC connection setup procedure to eNB2 (not shown in FIG. **2**).

[0040] Based on the identification of the D2D area where UE1 is currently located in, eNB2/DRSF2 may identify the eNB1/DRSF1 which is serving the UE1, at **230**. For example, eNB2 is able to identify the eNB ID based on the cell ID of UE1 provided by UE2, i.e. based on the leftmost 20 bit of the cell ID. Thus, eNB2/DRSF2 may obtain security context of UE1 from eNB1/DRSF1. As shown at **235**, eNB2/DRSF2 may send a request for UE1's UE-specific security key (e.g. $K_{d2d\text{-}UE1}$) to eNB1/DRSF1, indicating the S-TMSI of UE1. In response, eNB1/DRSF1 may identify the $K_{d2d\text{-}UE1}$ of UE1 based on the S-TMSI information of UE1 at **240**, and send this security key ($K_{d2d\text{-}UE1}$) to eNB2/DRSF2 at **245**.

[0041] Based on the received security context of UE1, the eNB2/DRSF2 may obtain keys for securing the D2D communications between UE1 and UE2. For example, the received security context of UE1 may comprise a particular sequence number, which may be mapped into one or more security keys indexed, for example, in the eNB2/DRSF2 or a database. Then, with the information of the security context of UE1, the eNB2/DRSF2 may identify or retrieve the matched keys for securing the D2D communications between UE1 and UE2. In some embodiments, the received security context of UE1 may comprise a UE-specific key $K_{d2d\text{-}UE1}$. Based on the $K_{d2d\text{-}UE1}$ and some security parameters, the eNB2/DRSF2 may generate or derive keys for securing the D2D communication to be performed between UE1 and UE2. For example, the keys for securing the D2D communication may be generated and distributed in a way as proposed in the related PCT patent application PCT/CN2013/078054, the contents of which are hereby incorporated by reference in its entirety. For example, eNB2/DRSF2 may generate a key K_{d2d_serv} based on the $K_{d2d\text{-}UE1}$ and a random number, and provide the K_{d2d_serv} to the UE2 together with the random number. The UE2 may store the K_{d2d_serv} as a security key for the D2D communication with UE1, and forward the random number to the UE1. With the received random number, the UE1 may derive the K_{d2d_serv} based on the $K_{d2d\text{-}UE1}$. As such, a common cryptography key, K_{d2d_serv} may be shared between the UE1 and the UE2 without interrupting the core network. In such a way, when the D2D UE pairs are served by different eNBs or in different D2D areas, it is still possible to obtain the D2D security keys for them UEs without involving core network side, even if the D2D UE pairs are in idle mode. This will relieve the burden of the core network greatly, especially in a case of large amounts of D2D users.

[0042] As discussed above, in some embodiments, the security context of a D2D UE may be transferred from a first eNB/DRSF to a second eNB/DRSF when the D2D UE is moving from a D2D area of the first eNB/DRSF to a D2D area of the second eNB/DRSF. FIG. **3** illustrates such an embodiment. As shown at **310** and **320**, UE1 may share a UE-specific key (e.g. $K_{d2d\text{-}UE1}$) for D2D services of UE1 with the eNB1/DRSF1 and the MME, for example, according to solutions defined in the PCT patent application PCT/CN2013/078054. For example, the key $K_{d2d\text{-}UE1}$ may be generated both at the UE1 and at the MME **132**, based on a NAS key (e.g. K_{asme} of